MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti minősített elektronikus bélyegző tanúsítvány szolgáltatási kivonat

ver. 2.21

Hatálybalépés: 2021-03-19

Azonosító	1.3.6.1.4.1.21528.2.1.1.194.2.21
Verzió	2.21
Első verzió hatálybalépése	2016-07-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2021-03-12
Hatálybalépés dátuma	2021-03-19

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1033 Budapest, Ángel Sanz Briz út 13.

Verzió	Hatálybalépés	A változás leírása
2.0	2016-07-01	- Új szabályzat az eIDAS szerint.
2.1	2016-09-05	- Módosítások az NMHH észrevételei alapján.
2.2	2016-10-30	- Módosítások a tanúsító észrevételei alapján.
2.3	2017-04-30	- Módosítások az NMHH észrevételei alapján.
2.4	2017-09-30	- Éves felülvizsgálat.
2.6	2018-03-24	- Teljes felülvizsgálat. - Közjegyzői személy azonosítás bevezetése. - Kisebb módosítások.
2.7	2018-09-15	- Éves felülvizsgálat.
2.8	2018-12-14	- Változások az auditor javaslatai alapján.
2.11	2019-09-25	- Éves felülvizsgálat.
2.12	2019-12-12	- Változások az auditor javaslatai alapján.
2.13	2020-03-05	- Hatály. - Időbélyegző tanúsítvány leírás módosítása. - Személyes azonosítás szabályai. - Tanúsítvány módosítás. - HSM követelmények. - Kisebb pontosítások.
2.14	2020-05-11	- Kisebb pontosítások. - Videotechnológiás természetes személy azonosítás bevezetése a 2.1.3 fejezetben. - A visszavonás feltételeinek kibővítése a 3.2 fejezetben.
2.15	2020-06-26	- Pontosítások a Távoli kulcsmenedzsment szolgáltatás kapcsán. - Videotechnológiás természetes személy azonosítás megszüntetése a 2.1.3 fejezetben. - Kisebb pontosítások.
2.16	2020-08-14	- OCSP Signing EKU eltávolítása a CA tanúsítványokból. - Kisebb pontosítások.
2.17	2020-10-28	- Pontosítások az auditor és a felügyelő hatóság észrevételei alapján. - Kisebb pontosítások.

Verzió	Hatálybalépés	A változás leírása
2.19	2020-12-28	- Videotechnológiás természetes személy azonosítás bevezetése a 2.1.3 fejezetben. - Szolgáltató által kezdeményezett Tanúsítvány megújítás szabályainak pontosítása. - Open Banking tanúsítványok bevezetése. - Kisebb módosítások.
2.21	2021-03-19	- MD 940 hozzáadása a MALE listához. - Kisebb módosítások.

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság (továbbiakban: Microsec vagy *Hitelesítés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató által meghatározott elektronikus bélyegző minősített tanúsítványának kibocsátása szolgáltatásra vonatkozó *Szolgáltatási kivonat*ot tartalmazza.

A *Szolgáltatási kivonat* a fogyasztók számára összefoglaló tájékoztatást tartalmaz a szolgáltatás igénybevételének feltételeiről a *Szolgáltatási szabályzat* rendelkezéseivel összhangban, a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet rendelkezései szerint.

A *Szolgáltatási kivonat* megfelel az eIDAS Rendelet [1] által támasztott követelményeknek, az ezen szabályoknak megfelelően nyújtott szolgáltatás a rendelet szerinti bizalmi szolgáltatás.

A *Hitelesítés-szolgáltató* a bizalmi szolgáltatás nyújtását 2016. július 1-jén jelentette be a Nemzeti Média- és Hírközlési Hatóságnak.

A minősített bizalmi szolgáltatások megfelelőségértékelését a TÜV Informationstechnik GmbH (továbbiakban TÜViT) végezte.

A sikeres megfelelőség értékelési vizsgálat alapján a Nemzeti Média- és Hírközlési Hatóság 2016. december 20-án nyilvántartásba vette és a nemzeti bizalmi listában publikálta a bejegyzett minősített bizalmi szolgáltatást.

A minősített bizalmi szolgáltatás megfelelőségértékelését független vizsgáló szervezetként 2020. októberétől a Hunguard Kft (továbbiakban Hunguard) végzi.

1.1. Dokumentum neve és azonosítója

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS Rendelet szerinti minősített elektronikus bélyegző tanúsítvány szolgáltatási kivonat
Dokumentum verziószáma	2.21
Hatálybalépés ideje	2021-03-19

A jelen *Szolgáltatási kivonat* szerint használható *Hitelesítési rend*ek felsorolását és azonosító adatait az 1.1.1 fejezet tartalmazza.

1.1.1. Hitelesítési rendek

A *Hitelesítés-szolgáltató* által kibocsátott valamennyi *Tanúsítvány* hivatkozik arra a *Hitelesítési rend*re, amely alapján a kibocsátás történt.

A jelen *Szolgáltatási kivonat* szerint a *Hitelesítés-szolgáltató* a következő *Hitelesítési rend*ek alapján bocsát ki *Tanúsítvány*okat:

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.181.2.21	Minősített, elektronikus bélyegző létrehozására és ellenőrzésére szolgáló, nem természetes személyek számára *Minősített elektronikus bélyegzőt létrehozó eszköz*ön kibocsátott *Tanúsítvány*okat szabályozó, álnevet kizáró hitelesítési rend.	MBJBN
1.3.6.1.4.1.21528.2.1.1.182.2.21	Minősített, elektronikus bélyegző létrehozására és ellenőrzésére szolgáló, nem természetes személyek számára *Hardver kriptográfiai eszköz*ön kibocsátott *Tanúsítvány*okat szabályozó, álnevet kizáró hitelesítési rend.	MBJHN
1.3.6.1.4.1.21528.2.1.1.183.2.21	Minősített, elektronikus bélyegző létrehozására és ellenőrzésére szolgáló, nem természetes személyek számára szoftveresen kibocsátott *Tanúsítvány*okat szabályozó, álnevet kizáró hitelesítési rend.	MBJSN

A *Hitelesítési rend*ek rövid nevének képzésének illetve értelmezésének szabályai a függelékben találhatóak.

A felsorolt *Hitelesítési rend*(ek) részletes követelményeit az " e-Szignó Hitelesítés Szolgáltató – eIDAS Rendelet szerinti minősített elektronikus bélyegző tanúsítvány hitelesítési rendek ver.2.21." [12] dokumentum tartalmazza.

Jelen *Hitelesítési rend*ek közül:

- valamennyi *Hitelesítési rend* megfelel az ETSI EN 319 411-2 [10] szabványban definiált [QCP-l] *Hitelesítési rend*nek;
- az [MBJBN] *Hitelesítési rend* megfelel a [QCP-l-qscd] *Hitelesítési rend*nek;
- az [MBJHN] *Hitelesítési rend* megfelel az ETSI EN 319 411-1 [9] szabványban definiált [NCP+] *Hitelesítési rend*nek.

Megfelelés az ETSI hitelesítési rendeknek

Amennyiben egy ETSI Hitelesítési Rend egy másik ETSI Hitelesítési Rendre épül, vagyis automatikusan tartalmazza annak valamennyi követelményét, a kibocsátott *Tanúsítvány*okban csak a magasabb szintű Hitelesítési Rend azonosítója kerül feltüntetésre.

	[QCP-l]	[QCP-l-qscd]	[NCP+]
MBJBN	(x)	X	
MBJHN	X		X
MBJSN	X		

1.2. Területi hatály

A jelen *Szolgáltatási kivonat* a magyar jog alapján Magyarországon, elsősorban magyar *Ügyfel*ek részére, magyar nyelven nyújtott szolgáltatásokra vonatkozó konkrét követelményeket tartalmaz. A *Hitelesítés-szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a magyar viszonyokra alkalmazható előírásoknak megfelelő, azoknál nem enyhébb követelményeket alkalmaz.

1.3. A bizalmi szolgáltató

1.3.1. A Szolgáltató adatai

Név:	Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
Cégjegyzékszám:	01-10-047218 Fővárosi Törvényszék Cégbírósága
Székhely:	1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	`https://www.microsec.hu`, `https://www.e-szigno.hu`

A *Hitelesítési rend*, a *Szolgáltatási szabályzat* és az Adatvédelmi szabályzat elérhetősége:

- `https://e-szigno.hu/dokumentumok-es-szabalyzatok`

Az árlista elérhetősége:

- `https://e-szigno.hu/arlista`

Díjvisszatérítés:

A Szolgáltatási szerződés megszűnése alapesetben az *Előfizető* által megfizetett díjakat nem érinti.

A már kifizetett díjakból a *Hitelesítés-szolgáltató* nem nyújt visszatérítést, kivéve, ha a Szolgáltatási szerződés a *Hitelesítés-szolgáltató* hibájából szűnik meg, vagy ha a *Hitelesítés-szolgáltató* ezt – például egyes csomagok esetében – kifejezetten lehetővé teszi.

A megfelelőségértékelési vizsgálatok tanúsítványai megtekinthetők a tanúsító szervezet publikus weboldalán [1]

illetve a *Hitelesítés-szolgáltató* saját weboldalán az alábbi linken:

`https://e-szigno.hu/eidas/eidas.html`

A magyar nemzeti bizalmi lista elérhetősége:

- humán olvasható PDF formátumban: `http://www.nmhh.hu/tl/pub/HU_TL.pdf`
- géppel feldolgozható XML formátumban: `http://www.nmhh.hu/tl/pub/HU_TL.xml`

A Nemzeti Média- és Hírközlési Hatóság bizalmi szolgáltatásokkal kapcsolatos nyilvántartása az alábbi elérhetőségen található:

http://webpub-ext.nmhh.hu/esign2016/

Szolgáltatási szerződés elérhetősége:

A *Hitelesítés-szolgáltató* az *Ügyfel*ekkel kötendő Szolgáltatási szerződést az *Igénylő* kezdeti regisztráció alkalmával megadott értesítési e-mail címére továbbítja.

[1] `https://www.hunguard.hu/ugyfeleinknek/tanusitott-termekek-rendszerek/eidas-rendelet-szerinti-bizalmi-szolgaltatas/microsec-zrt/`

1.3.2. Az ügyfélszolgálati iroda elérhetősége

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	
	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park Déli Terüet, C épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 8:30-16:30 között előzetes időpont egyeztetés alapján
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda email címe:	`info@e-szigno.hu`
Visszavonási kérelmek fogadása:	`visszavonas@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`https://www.e-szigno.hu`
Panaszok bejelentésének helye:	Microsec zrt.
	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park Déli Terület, C épület
Illetékes fogyasztóvédelmi felügyelőség:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 144.
Illetékes békéltető testület elérhetősége:	Budapesti Békéltető Testület 1016 Budapest, Krisztina krt. 99. III. em. 310. Levelezési cím: 1253 Budapest, Pf.: 10.

1.4. Tanúsítványfajták

A elektronikus bélyegző minősített tanúsítványának kibocsátása szolgálatáshoz tartozó *Szolgáltatási szabályzat* által támogatott *Hitelesítési rend*eket a *Szolgáltatási szabályzat* 1.2.1 fejezete mutatja be. Az alkalmazott *Hitelesítési rend* azonosítója minden esetben feltüntetésre kerül a *Tanúsítvány* "Certificate Policies" mezejében.

Az e-Szignó Hitelesítés Szolgáltató több különböző tanúsítványfajtát kínál *Ügyfel*ei részére, amelyek főképp az általuk hitelesen az *Alany*hoz kötött adatok és tulajdonságok körében térnek el:

- *Szervezeti tanúsítvány*ról beszélünk, ha a *Tanúsítvány* alanya *Szervezet*, a *Szervezet* irányítása alatt álló eszköz, vagy ha a *Tanúsítvány* egy természetes személy *Alany* valamely *Szervezet*hez való tartozását mutatja. Ilyen esetben a *Tanúsítvány* "O" mezejében a *Szervezet* neve feltüntetésre kerül. Az ilyen *Tanúsítvány* kizárólag az adott *Szervezet* által

meghatározott módon használható. Természetes személy számára kibocsátott *Szervezeti tanúsítvány* esetén a "Title" mezőben további korlátozások szerepelhetnek a *Tanúsítvány* használhatóságával kapcsolatban.

- *Automata tanúsítvány*ról beszélünk, ha a *Tanúsítvány*ban az *Alany* adatai között feltüntetésre kerül az informatikai eszköz (alkalmazás, rendszer) elnevezése is, amely segítségével az *Alany* a *Tanúsítvány*t használja.
- Álneves *Tanúsítvány*ról beszélünk, ha a *Tanúsítvány*ban nem az *Alany* közhiteles nyilvántartásban szereplő hivatalos elnevezése szerepel. Az álneves *Tanúsítvány*okban a kért elnevezés a "Pseudonym" mezőben kerül feltüntetésre, és a "CN" mezőben feltüntetésre kerül, hogy a *Tanúsítvány* álnevet tartalmaz.
- *Minősített elektronikus bélyegzőt létrehozó eszköz* használatát megkövetelő *Tanúsítvány*ok: Abban az esetben, ha a *Tanúsítvány* egy olyan nyilvános kulcshoz lett kibocsátva, amelyhez tartozó magánkulcs egy *Minősített elektronikus bélyegzőt létrehozó eszköz*ön lett generálva -– azaz garantált, hogy a magánkulcs onnan nem kinyerhető, nem másolható –, akkor a *Tanúsítvány*ban is feltüntetésre kerül ez az információ a "QCStatements" mezőben. Minősített elektronikus bélyegző csak ilyen *Tanúsítvány* alapján készíthető.
- Személyes *Tanúsítvány*ról akkor beszélhetünk, ha a *Tanúsítvány* sem "O", sem "Title" mezőt nem tartalmaz. Ilyen csak természetes személyek számára kerül kibocsátásra.

Az e-Szignó Hitelesítés Szolgáltató mind természetes személyek, mind jogi személyek számára bocsát ki *Tanúsítvány*okat. Jogi személyek számára igényelt *Tanúsítvány*ok esetében a képviseletre jogosult természetes személynek vagy az általa meghatalmazott személynek kell eljárnia a *Tanúsítvány* ügyében.

1.5. A tanúsítvány felhasználhatósága

1.5.1. Megfelelő tanúsítvány használat

A *Hitelesítés-szolgáltató* által jelen szolgáltatás keretében kibocsátott végfelhasználói *Tanúsítvány*okhoz tartozó magánkulcsok kizárólag elektronikus bélyegző előállítására használhatóak fel, a *Tanúsítvány*ok segítségével az elektronikus bélyegző létrehozója igazolhatja az általa lebélyegzett elektronikus dokumentumok hitelességét.

A *Tanúsítvány*ban szereplő nyilvános kulcs, maga a *Tanúsítvány*, a *Tanúsítvány visszavonási list*ák, az *Időbélyegző*k és az online tanúsítvány-állapot válaszok az elektronikus bélyegző ellenőrzésére használhatók fel.

1.5.2. Tiltott tanúsítvány használat

A jelen *Szolgáltatási kivonat* alapján kibocsátott *Tanúsítvány*okat, illetve a hozzájuk tartozó magánkulcsokat elektronikus bélyegző előállításától illetve ellenőrzésétől eltérő célra felhasználni tilos.

1.6. Felügyeleti szerv

A *Szolgáltatási szabályzat*ok és a szolgáltatások nyújtása feletti felügyeletet a Nemzeti Média- és Hírközlési Hatóság látja el. A Nemzeti Média- és Hírközlési Hatóság nyilvántartást vezet a követelményeknek megfelelő *Hitelesítési rend*ekről valamint az ezeket alkalmazó *Hitelesítés-szolgáltató*król.

A Nemzeti Média- és Hírközlési Hatóság bizalmi szolgáltatásokkal kapcsolatos nyilvántartása az alábbi elérhetőségen található:

`http://webpub-ext.nmhh.hu/esign2016/`

2. Azonosítás és hitelesítés

2.1. Kezdeti regisztráció, azonosság hitelesítése

A *Hitelesítés-szolgáltató* a törvény által biztosított keretek között tetszőleges kommunikációs csatornát felhasználhat a *Tanúsítvány*t kérelmező személy vagy szervezet azonosságának igazolására, a megadott adatok valódiságának ellenőrzésére.

A *Hitelesítés-szolgáltató* saját hatáskörében, külön indoklás nélkül

megtagadhatja az igényelt *Tanúsítvány* kibocsátását.

2.1.1. A magánkulcs birtoklásának igazolása

A *Tanúsítvány* kiállítása előtt a *Hitelesítés-szolgáltató* biztosítja illetve meggyőződik arról, hogy az *Igénylő* valóban birtokolja illetve ellenőrzése alatt tartja a *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulcsot.

Amennyiben az *Alany* számára a minősített *Tanúsítvány*hoz tartozó magánkulcsot a *Hitelesítés-szolgáltató* saját szervezetén belül maga generálja – jellemzően a *Minősített elektronikus bélyegzőt létrehozó eszköz* vagy *Hardver kriptográfiai eszköz* használatát megkövetelő *Hitelesítési rend*ek esetén – , akkor nem kell külön ellenőriznie azt, hogy az *Igénylő* rendelkezik-e a hitelesítendő nyilvános kulcs magánkulcs-párjával.

Amennyiben az *Igénylő* általa biztosított kulcshoz kéri a *Tanúsítvány* kibocsátását – jellemzően szoftveres tanúsítványok esetében –, akkor a *Hitelesítés-szolgáltató* PKCS#10 formátumban fo-

gadja a *Tanúsítványkérelmet*, amely egyúttal igazolja, hogy valóban a magánkulcs birtokosa kért *Tanúsítvány*t az adott megnevezéshez.

Amennyiben az *Alany* magánkulcsát egy másik *Bizalmi szolgáltató* generálja és kezeli, akkor a *Hitelesítés-szolgáltató* meggyőződik arról, hogy a magánkulcs az említett *Bizalmi szolgáltató* birtokában van, és az *Alany* kizárólagos ellenőrzése alatt áll. A *Hitelesítés-szolgáltató* elfogadhatja az említett *Bizalmi szolgáltató* erről szóló hiteles nyilatkozatát. A nyilatkozat formája lehet elektronikus. A nyilatkozat hitelességét a *Hitelesítés-szolgáltató* ellenőrzi. A birtoklás ellenőrzése PKCS#10 formátumú *Tanúsítványkérelem* befogadásával történik.

2.1.2. Szervezet azonosságának hitelesítése

A *Szervezet* azonossága ellenőrzésre kerül a következő esetekben:

- amennyiben a kibocsátandó *Tanúsítvány* alanya a *Szervezet*;
- amennyiben a kibocsátandó *Tanúsítvány* alanya a *Szervezet* által üzemeltetett eszköz vagy rendszer;

*Szervezeti tanúsítvány*ok kibocsátása előtt a *Hitelesítés-szolgáltató* egy közhiteles nyilvántartás alapján meggyőződik a *Tanúsítvány*ba kerülő szervezeti adatok valódiságáról.

Ezekben az esetekben ellenőrzésre kerül továbbá, hogy:

- a *Szervezet* nevében eljáró természetes személy jogosult-e a *Szervezet* nevében eljárni;
- a *Szervezet* hozzájárult-e a *Tanúsítvány* kibocsátásához.

Az ellenőrzés elvégzéséhez az *Ügyfél*nek a következő adatokat kell megadnia:

- a *Szervezet* hivatalos elnevezése, székhelye és jogállása;
- a *Szervezet* hivatalos nyilvántartási száma (pl. cégjegyzékszám, adószám), ha van ilyen;
- a *Szervezet*en belüli szervezeti egység neve, ha kérik ennek feltüntetését a *Tanúsítvány*ban;
- Amennyiben az *Ügyfél* kéri az *Alany* Open Banking követelmények, vagy a módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatainak feltüntetését a *Tanúsítvány*ban, akkor az *Ügyfél*nek meg kell adnia az *Alany* pénzforgalmi szolgáltatásait felügyelő hatóság által kiosztott engedélyszámát vagy annak hiányában a hatóság által elismert egyéb azonosítóját, a pénzforgalmi szolgáltatásainak típusát, valamint az említett hatóság nevét.

A *Tanúsítványkérelem*hez csatolni kell a következő igazolásokat illetve bizonyítékokat:

- a kérelem benyújtója által aláírt nyilatkozatot arról, hogy a *Szervezet* azonosítására megadott adatok helyesek és megfelelnek a valóságnak;
- a kérelem benyújtója által aláírt nyilatkozatot arról, hogy a *Szervezet Tanúsítvány*ban feltüntetendő adatai között nem szerepel védjegy, vagy amennyiben szerepel, igazolást arról, hogy a védjegy használatára a *Szervezet* jogosult;
- igazolást arra vonatkozóan, hogy a *Szervezet* nevében *Tanúsítványkérelmet* benyújtó természetes személy jogosult a kérelmet benyújtani [2];
- a *Szervezet* képviseletére jogosult személy aláírási címpéldányát vagy más, az aláírási címpéldánnyal egyenértékű hivatalos dokumentumot, mely a *Szervezet* képviseletére jogosult személyek nevét és aláírását tartalmazza [3];
- a *Szervezet* létezését, elnevezését és jogállását hitelesítő dokumentumot [4].

A *Hitelesítés-szolgáltató* a bemutatott iratok és okmányok érvényességét és hitelességét ellenőrzi.

Külföldön bejegyzett Szervezetek azonosságának ellenőrzése

A *Hitelesítés-szolgáltató* külföldön bejegyzett *Szervezet*ek azonosítását sem zárja ki, amennyiben megvalósítható az adott ország megfelelő nyilvántartásaival való adategyeztetés vagy megbízható harmadik fél által kiadott igazolás beszerzése.

Az adategyeztetés tekintetében a *Hitelesítés-szolgáltató* elfogadja:

- a külföldi ország kormányzati nyilvántartásából a *Hitelesítés-szolgáltató* által közvetlenül beszerzett, vagy harmadik fél által lekérdezett, de az elsődleges adatszolgáltató által hitelesített információt;
- a külföldi ország magyarországi nagykövetsége vagy konzulátusa által kibocsátott igazolást, miszerint az adott szervezet létezik és a megadott adatai helyesek;
- a külföldi országban lévő magyar nagykövetség vagy konzulátus által kibocsátott igazolást, miszerint az adott szervezet létezik és a megadott adatai helyesek.

A *Hitelesítés-szolgáltató* egyéb okmányokat és bizonyítékokat is elfogadhat, amennyiben meggyőződik róla, hogy az a fentiekkel megegyező szintű biztonságot jelentenek. Ezen bizonyítékok beszerzése és a *Hitelesítés-szolgáltató*hoz történő eljuttatása az *Ügyfél* feladata.

A *Hitelesítés-szolgáltató* kizárólag érvényes okmányokat, illetve 3 hónapnál nem régebbi bizonyítékokat fogad el.

[2] A felhatalmazások, jogosultságok ellenőrzésével kapcsolatos részleteket a 2.1.5. fejezet tartalmazza.
[3] Cégbíróságon bejegyzett cégek esetében a fenti iratokat a *Hitelesítés-szolgáltató* is beszerezheti.
[4] Cégbíróságon bejegyzett cégek esetében a fenti iratokat a *Hitelesítés-szolgáltató* is beszerezheti.

A *Hitelesítés-szolgáltató* nem állítja ki a *Tanúsítvány*t, amennyiben belső szabályzatai alapján úgy ítéli meg, hogy nem képes a külföldön kiállított igazolást, okmányt vagy a külföldi szervezet adatait megfelelő biztonsággal ellenőrizni.

A *Hitelesítés-szolgáltató* a bizalmi szerepkörök megfelelő elosztásával és belső adminisztratív folyamatainak segítségével biztosítja, hogy a szervezeti adatok rögzítése és az adatok hitelességének ellenőrzése során legalább két - bizalmi szerepkört ellátó - alkalmazott részvételére van szükség.

2.1.3. Természetes személy azonosságának hitelesítése

A természetes személy azonosságát igazolni kell:

- amennyiben a természetes személy egy *Szervezet* nevében jár el *Szervezeti tanúsítvány* kérelmezése céljából.

Minősített *Tanúsítvány* kibocsátásakor a természetes személy azonosságát az eIDAS Rendelet [1] 24. cikk (1) bekezdése értelmében személyes jelenlét útján vagy azzal egyenértékű biztosítékot nyújtó módszerrel kell ellenőrizni. A *Hitelesítés-szolgáltató* a 24. cikk (1) bekezdésben leírt azonosítási módokat alkalmazza az alábbiak szerint.

A *Hitelesítés-szolgáltató* a természetes személy azonosságát az alábbi lehetőségek valamelyikének alkalmazásával ellenőrzi.

1. **Személyesen történő azonosítás során.**
   - A természetes személynek személyesen meg kell jelennie a személyes azonosítást végző személy előtt, aki az alábbiak valamelyike lehet:
     - *Regisztráló szervezet* tisztviselője,
     - közjegyző, mint harmadik fél a magyar szabályozás szerint.
   - A személyes azonosítás során a természetes személy azonossága ellenőrzésre kerül egy személyazonosság igazolására alkalmas hatósági igazolványa alapján.

     Az azonosítás az alábbi hatósági igazolványok alapján történik:
     - a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (a továbbiakban: Nytv. [3]) hatálya alá tartozó természetes személyek esetében a Nytv. szerinti személyazonosság igazolására alkalmas hatósági igazolvány az Eüt. 82.§ (3) [5] szerint;
     - a Nytv. [3] hatálya alá nem tartozó természetes személy esetén a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról, illetve a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény [4] szerinti úti okmány alapján az Eüt. 82.§ (4) [5] szerint;

  - a fenti okmányok egyikével sem rendelkező természetes személyek azonosítása során a *Hitelesítés-szolgáltató* csak európai állampolgárok azonosságának ellenőrzése esetében alkalmazza az Eüt. 82.§ (5) [5] bekezdése szerinti személyazonosság ellenőrzést. Ebben az esetben a természetes személy állampolgársága szerinti európai ország által kibocsátott fényképes személyi igazolványt fogadja el, mint személyazonosság igazolására szolgáló megbízható okmányt.

- A személyazonosság ellenőrzésére szolgáló adatok helyességét a természetes személynek papír alapú írásos nyilatkozatban, saját kezű - az azonosítást végző személy jelenlétében létrehozott - aláírásával igazolnia kell.
- A személyes azonosítást végző személy ellenőrzi, hogy a bemutatott igazolványokon történt-e módosítás vagy hamisítás.

A *Hitelesítés-szolgáltató* a kezdeti azonosítás során a saját *Regisztráló szervezet*e által végzett azonosítással egyenértékűnek fogadja el a közjegyző által végzett természetes személy azonosítást.

Külföldi állampolgárok személyazonosság ellenőrzésének további szabályai

A *Hitelesítés-szolgáltató* olyan külföldi ország közjegyzője által végzett azonosítást ismer el a saját *Regisztráló szervezet*e által végzett azonosítással egyenértékűnek,

- amely külföldi országgal Magyarország a közokiratok kölcsönös elismeréséről szóló kétoldalú nemzetközi egyezményt kötött, vagy
- amely külföldi ország aláírta a külföldön felhasználásra kerülő közokiratok diplomáciai vagy konzuli hitelesítésének (felülhitelesítésének) mellőzéséről Hágában, 1961. október 5. napján kelt egyezményt (Apostille)

A közjegyző által kiállított dokumentumokat az adott egyezmény által megkövetelt formátumban és tartalommal kell benyújtani.

A *Hitelesítés-szolgáltató* akkor fogadja el a külföldi ország közjegyzője előtt aláírt *Tanúsítványkérelmet*, ha a közjegyzői záradékból kitűnik, hogy

- a közjegyző egy hivatalos személyazonosító okmány (személyi igazolvány, útlevél stb.) alapján azonosította az *Igénylő* természetes személyt;
- az *Igénylő* a közjegyző jelenlétében írta alá a *Tanúsítványkérelmet*.

A *Hitelesítés-szolgáltató* minden esetben elfogadja a magyar vagy angol nyelven kiállított eredeti dokumentumokat. Egyéb nyelven kiállított dokumentumok esetében a *Hitelesítés-szolgáltató* kérheti a dokumentumok hiteles - az Országos Fordító és Fordításhitelesítő Iroda (OFFI) által készített - magyar nyelvű fordítását.

A *Hitelesítés-szolgáltató* egyéb okmányokat és bizonyítékokat is elfogadhat, amennyiben meggyőződik róla, hogy az a fentiekkel megegyező szintű biztonságot jelentenek. Ezen bizonyítékok beszerzése és a *Hitelesítés-szolgáltató*hoz történő eljuttatása az *Ügyfél* feladata.

A *Hitelesítés-szolgáltató* kizárólag érvényes okmányokat, illetve 3 hónapnál nem régebbi bizonyítékokat fogad el.

A *Hitelesítés-szolgáltató* nem állítja ki a *Tanúsítvány*t, amennyiben belső szabályzatai alapján úgy ítéli meg, hogy nem képes valamely bemutatott okmányt vagy a személy adatait megfelelő biztonsággal ellenőrizni.

2. **Elektronikus aláírás vagy elektronikus bélyegző tanúsítványára visszavezetett azonosítással.**

   Ebben az esetben:

   - Az *Igénylő* a *Tanúsítványkérelmet* elektronikus formában nyújtja be egy nem álneves minősített *Tanúsítvány*án alapuló minősített elektronikus aláírással vagy minősített elektronikus bélyegzővel ellátva.
   - Az elektronikus aláírással ellátott *Tanúsítványkérelem*nek tartalmaznia kell a természetes személy egyértelmű azonosításához szükséges azonosító adatokat.
   - A *Tanúsítványkérelem* hitelességét és sértetlenségét ellenőrizni kell a teljes tanúsítási lánc vizsgálatával.
   - A *Hitelesítés-szolgáltató* csak olyan *Tanúsítvány*on alapuló elektronikus aláírást vagy elektronikus bélyegzőt fogad be, amelyet egy az Európai Uniós fő bizalmi listán publikált nemzeti bizalmi listán szereplő bizalmi szolgáltatás keretében bocsátottak ki, és az aláírás vagy bélyegző létrehozás időpontjában érvényes volt.
   - A *Hitelesítés-szolgáltató* csak olyan *Tanúsítvány*on alapuló elektronikus aláírást fogad be, amelyet az eIDAS Rendelet [1] 24. cikk (1) bekezdése (a) vagy (b) pontja szerinti személy azonosítás alapján bocsátottak ki.

3. **Nemzeti szinten elismert egyéb azonosítási módszer alkalmazásával**

   A *Hitelesítés-szolgáltató* a természetes személy azonosságának megállapítását a személyes találkozással egyenértékűnek elismert videotechnológiát biztosító elektronikus hírközlő eszköz útján történő azonosítás (a továbbiakban: videotechnológiás azonosítás) felhasználásával is elvégezheti az 541/2020. (XII. 2.) Kormány rendelet [6] szerint.

   Ebben az esetben a *Hitelesítés-szolgáltató* a személyesen történő azonosítás során előírtak szerint jár el azzal a különbséggel, hogy a személyes találkozást olyan videotechnológiás azonosítási eljárással váltja ki, amely során:

(a) élő telekommunikációs kapcsolat során videofelvétel útján képmást készít az *Ügyfél*ről, majd összeveti az *Ügyfél*ről készített fényképet és az azonosításhoz felhasznált személyazonosság igazolására alkalmas okmányban (a továbbiakban: okmány) szereplő képmást. Az azonosítás akkor megfelelő, ha a *Hitelesítés-szolgáltató* által egyértelműen megállapítható, hogy az okmányban szereplő személy azonos a videofelvételen szereplő *Ügyfél*lel.

(b) A *Hitelesítés-szolgáltató* a "Tájékoztató az online videóazonosítás feltételeiről" [13] dokumentumban részletesen meghatározza a videótechnológiás azonosítás igénybevételének feltételeit, különösen a videókapcsolat minőségének minimális követelményeit. A dokumentum a nyilvános szabályzatok között publikálásra kerül a *Hitelesítés-szolgáltató* web oldalán.

A sikeres videotechnológiás azonosítás érdekében célszerű biztosítani az alábbi feltételeket:

- jó állapotban lévő okmány
- megfelelően megvilágított környezet
- csendes, zavarmentes környezet
- idegen személyek jelenlétének kizárása
- IT eszköz kétirányú hang és videó képességgel
- kamera min. 2 megapixel video felbontással
- stabil internetkapcsolat min 1,5Mbps sebességgel.

(c) A *Hitelesítés-szolgáltató* a *Szolgáltatási szabályzat* és a "Tájékoztató az online videóazonosítás feltételeiről" [13] dokumentum bemutatásával és a videofelvétel során biztosítja, hogy az *Ügyfél* a videotechnológiás azonosítás feltételeit részletesen megismerhesse, és azok betartásához kifejezetten hozzájárult, aszerint jár el.

(d) A *Hitelesítés-szolgáltató* a videotechnológiás azonosítás során a *Hitelesítés-szolgáltató* és az *Ügyfél* között létrejött teljes kommunikációt, az *Ügyfél* videotechnológiás azonosítással kapcsolatos részletes tájékoztatását és az *Ügyfél* ehhez történő kifejezett hozzájárulását visszakereshető módon, kép- és hangfelvételen – a kép- és hangfelvétel minőségének romlását kizáró módon – rögzíti, és azt a felvételtől számított legalább 10 évig megőrzi.

(e) A sikeres videotechnológiás azonosítás feltétele, hogy a videotechnológiás azonosítást lehetővé tévő elektronikus hírközlő eszköz képfelbontása és a kép megvilágítása alkalmas legyen az *Ügyfél* nemének, korának, arcjellemzőinek felismerésére, valamint az *Ügyfél*

- úgy nézzen bele a kamerába, hogy arcképe felismerhető és rögzíthető legyen, valamint azonosítható legyen az általa bemutatott okmányon látható arckép alapján,

- érthető módon közölje a videotechnológiás azonosításhoz használt okmány azonosítóját,
- úgy mutassa az okmányát, hogy az azon található biztonsági elemek és adatsorok felismerhetőek, rögzíthetőek és ellenőrizhetőek legyenek, valamint
- okmányán megtalálható adatok megfeleltethetők az *Ügyfél*ről a *Hitelesítés-szolgáltató*nál rendelkezésre álló adatokkal, és az *Ügyfél* a képmása alapján az okmányon felmutatott képmással azonosítható.

(f) A *Hitelesítés-szolgáltató* megbizonyosodik arról, hogy az okmány alkalmas a videotechnológiás azonosítás elvégzésére, így

- az okmány megfelel az okmányt kiállító hatóság előírásainak,
- az egyes biztonsági elemek – különösen a hologram, a kinegram vagy ezekkel megegyező más biztonsági elemek – felismerhetőek és sérülésmentesek, és
- az okmány azonosítója megegyezik az *Ügyfél* által közölt okmányazonosítóval, felismerhető és sérülésmentes.

(g) A videotechnológiás azonosítás során a *Hitelesítés-szolgáltató* megbizonyosodik arról, hogy

- az *Ügyfél* arcképe felismerhető és azonosítható az általa bemutatott okmányon látható arckép alapján, és
- az okmányon megtalálható adatok logikailag megfeleltethetők az *Ügyfél*ről a *Hitelesítés-szolgáltató*nál rendelkezésre álló adatokkal.

(h) Az élő telekommunikációs kapcsolatnak megfelel az is, ha a feltételek vizsgálatát a *Hitelesítés-szolgáltató* gépi úton vagy a telekommunikációs kapcsolat megszűnését követően végzi el, de meggyőződik arról, hogy az *Ügyfél* az azonosítás során élő kapcsolatban van.

A *Hitelesítés-szolgáltató* csak abban az esetben bocsátja ki a *Tanúsítvány*t, ha a videotechnológiás azonosítás maradéktalanul megfelel a fenti követelményeknek.

A Szolgáltatási szerződés érvényességének időtartama alatt, amennyiben az *Igénylő* a lejárt vagy visszavont *Tanúsítvány*a helyett újat igényel, vagy a meglevő *Tanúsítvány*a mellé újabb *Tanúsítvány*t igényel ugyanazon Szolgáltatási szerződés keretében, akkor a *Hitelesítés-szolgáltató* felhasználja a korábbi személy azonosítás során egyeztetett adatokat. A *Tanúsítványkérelem* hitelességét, a *Tanúsítvány*ba kerülő adatok érvényességét és az *Igénylő* személyazonosságát a *Hitelesítés-szolgáltató* ilyen esetben is ellenőrzi.

A *Hitelesítés-szolgáltató* a bizalmi szerepkörök megfelelő elosztásával és belső adminisztratív folyamatainak segítségével biztosítja, hogy a személyes adatok rögzítése és az adatok hitelességének ellenőrzése során legalább két - bizalmi szerepkört ellátó - alkalmazott részvételére van szükség.

2.1.4. Nem ellenőrzött alany információk

A *Hitelesítés-szolgáltató* által kibocsátott *Tanúsítvány*ba csak olyan adatok kerülnek, amelyeket a *Hitelesítés-szolgáltató* ellenőrzött.

2.1.5. Jogok, felhatalmazások ellenőrzése

Szervezeti tanúsítvány kiállítása előtt a *Szervezet* nevében eljáró természetes személy azonosságát igazolni kell a 2.1.3. fejezet előírásai szerint.

Ellenőrizni kell a természetes személy képviseleti jogosultságát.

Egy *Szervezet* nevében eljárhat:

- az adott *Szervezet* képviseletére jogosult természetes személy;
- aki az adott *Szervezet* képviseletére jogosult személytől erre a célra meghatalmazással rendelkezik;
- az adott *Szervezet* képviseletére jogosult személy által kijelölt *Szervezeti ügyintéző*.

A *Szervezeti ügyintéző* kijelölhető a tanúsítvány igénylés során, vagy később is bármikor a megfelelő formanyomtatvány segítségével. Az űrlapon meg kell adni a kijelölt személy(ek) azonosító adatait, amelyek alapján a későbbi eljárás során azonosíthatóak. Az űrlapot a *Szervezet* képviselőjének (saját kezű vagy nem álneves tanúsítványon alapuló minősített elektronikus) aláírással kell ellátnia, amelyet az űrlap befogadásakor a *Hitelesítés-szolgáltató* regisztrációs munkatársai ellenőriznek.

Szervezeti ügyintéző kijelölése nem kötelező, illetve egyidejűleg több *Szervezeti ügyintéző* is kijelölhető. Amennyiben nincs kijelölve *Szervezeti ügyintéző*, akkor az adott szervezet képviseletére jogosult személy láthatja el ezt a feladatot.

2.1.6. Együttműködési képességre vonatkozó követelmények

A *Hitelesítés-szolgáltató* a szolgáltatás nyújtása során nem működik együtt más *Hitelesítés-szolgáltató*kkal.

2.1.7. Email cím megerősítése

A *Hitelesítés-szolgáltató* weboldalán benyújtott kérelmek esetében a *Tanúsítványkérelem* űrlap kitöltése előtt a *Hitelesítés-szolgáltató* validálja az *Igénylő* email címét az email cím feletti kontroll ellenőrzésével. A weboldal az űrlap kitöltése előtt kéri az *Igénylő* email címének megadását és nem enged más adatot kitölteni. A *Hitelesítés-szolgáltató* a megadott email címre kiküld egy véletlenszámot is tartalmazó, korlátozott érvényességi idejű, igénylésenként egyedi URL-t. Az *Igénylő*

csak a kapott egyedi linkre kattintva tudja folytatni az űrlap kitöltését. A beérkező *Tanúsítványkérelem*hez így minden esetben tartozik egy - a működés során ellenőrzött - email cím.

Egyéb módon benyújtott *Tanúsítványkérelem* esetében a *Hitelesítés-szolgáltató* egy véletlenszámot is tartalmazó email-t küld az ellenőrzendő email címre. Az *Igénylő*-nek egy válasz email küldésével kell megerősítenie az igénylést. A válasz emailnek tartalmaznia kell a *Hitelesítés-szolgáltató* által küldött véletlenszámot. A véletlenszám érvényességi ideje 30 nap.

2.2. Adatvédelmi szabályzat

A *Hitelesítés-szolgáltató* az *Ügyfél*ek adatait a jogi előírásoknak megfelelően kezeli. Az Adatvédelmi szabályzat elérhető a *Hitelesítés-szolgáltató* honlapján

(`https://e-szigno.hu/minden-dokumentum.html`),

további információ a *Szolgáltatási szabályzat* 9.3 pontjában olvasható.

3. A tanúsítványokra vonatkozó követelmények

3.1. A kulcspár és a tanúsítvány használata

3.1.1. A magánkulcs és a tanúsítvány használata

Az *Alany* a *Tanúsítvány*ához tartozó magánkulcsát kizárólag elektronikus bélyegző létrehozására használhatja, más felhasználás nem engedélyezett.

Lejárt érvényességű, visszavont, vagy felfüggesztett *Tanúsítvány*hoz tartozó magánkulcs nem használható elektronikus bélyegző létrehozására.

Az *Alany* köteles gondoskodni magánkulcsának és aktivizáló adatának megfelelő védelméről.

A használat során be kell tartani az 1.5. fejezetben leírt korlátozásokat.

3.1.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

A *Tanúsítvány* segítségével igazolt elektronikus bélyegző elfogadása során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához ajánlott, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, különös tekintettel az alábbiakra:

- ellenőrizze a *Tanúsítvány* érvényességét és visszavonási állapotát;
- a bélyegző *Tanúsítvány*okat, illetve az azokhoz tartozó nyilvános kulcsokat kizárólag elektronikus bélyegző ellenőrzésére használja;
- a *Tanúsítvány*ra vonatkozó ellenőrzéseket célszerű elvégeznie a teljes tanúsítványláncra vonatkozóan egy megbízható gyökér vagy köztes szolgáltatói tanúsítványig;

- a tanúsítványlánc felépítésekor megbízható kibocsátó (bizalmi horgony) gyanánt olyan bizalmi szolgáltatói *Tanúsítvány*t fogadjon el, amely
  - minősített végfelhasználói *Tanúsítvány*ok kibocsátására jogosult bizalmi szolgáltatásként szerepel a magyar bizalmi listában [11], és
  - tartozik hozzá olyan szolgáltatói *Tanúsítvány*, amely érvényes volt a bélyegző létrehozásának időpontjában és a bélyegző létrehozására használt végfelhasználói *Tanúsítvány* kibocsátásának időpontjában;
- az elektronikus bélyegző ellenőrzését megbízható alkalmazással végezze, amely megfelel az aktuális vonatkozó műszaki ajánlásoknak, és amely rugalmasan konfigurálható és megfelelően van beállítva, valamint vírusmentes környezetben fut;
- javasolt ellenőrizni, hogy a *Tanúsítvány* a célnak megfelelő *Hitelesítési rend* alapján lett-e kibocsátva;
- minősített elektronikus bélyegző elfogadásakor javasolt ellenőrizni, hogy a *Tanúsítvány Minősített elektronikus bélyegzőt létrehozó eszköz* használatát előíró *Hitelesítési rend* alapján lett-e kibocsátva;
- amennyiben a *Tanúsítvány*ban feltüntetésre kerül, javasolt megvizsgálni a Tanúsítvánnyal egy alkalommal vállalható kötelezettség legmagasabb értékét (az ezen korlátokat meghaladó ügyletekben kibocsátott és lebélyegzett elektronikus dokumentumból származó követelésekért, illetve az így okozott kárért a *Hitelesítés-szolgáltató* nem felel);
- vegyen figyelembe minden korlátozást, amely a *Tanúsítvány*ban vagy a *Tanúsítvány*ban meghivatkozott szabályzatokban szerepel.

A *Hitelesítés-szolgáltató* elérhetővé tesz olyan szolgáltatást az *Ügyfel*ei és az *Érintett felek* számára, amely segítségével ellenőrizhetik az általa kibocsátott *Tanúsítvány*okat.

3.2. Tanúsítvány visszavonás és felfüggesztés

A tanúsítvány visszavonás alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* a *Tanúsítvány* érvényességét megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont *Tanúsítvány* már soha többé nem lehet újra érvényes.

A tanúsítvány felfüggesztés alatt azt a folyamatot értjük, amikor a *Hitelesítés-szolgáltató* egy még érvényes *Tanúsítvány* érvényességét átmenetileg megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány felfüggesztés egy átmeneti állapot, a felfüggesztett *Tanúsítvány*

visszavonható, vagy a *Tanúsítvány* eredeti érvényességi idejének lejárta előtt a felfüggesztés visszavonásával újra érvényessé tehető. A felfüggesztés visszavonása esetén a *Tanúsítvány* érvényessé válik visszamenőleges hatállyal, mintha a felfüggesztés meg sem történt volna.

A visszavont és felfüggesztett *Tanúsítvány*hoz tartozó magánkulcs használatát azonnal meg kell szüntetni, illetve fel kell függeszteni.

A visszavont *Tanúsítvány*hoz tartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges.

Felelősségi szabályok a felfüggesztéssel és visszavonással kapcsolatban:

- Amennyiben a *Hitelesítés-szolgáltató* már közzétette a *Tanúsítvány* visszavont állapotát, a *Hitelesítés-szolgáltató* semmilyen felelősséget nem vállal azért, ha az *Érintett fél* a közzétételt követően érvényesnek tekinti a *Tanúsítvány*t.

3.2.1. Ki kérelmezheti a visszavonást

A *Tanúsítvány* visszavonását kezdeményezhetik az *Ügyfel*ek, részletezve:

- az *Előfizető*;
- az *Előfizető* által bejelentett *Szervezeti ügyintéző*;
- az *Alany* pénzforgalmi szolgáltatási engedélyét kibocsátó hatóság, amennyiben a *Tanúsítvány* az *Alany* Open Banking követelmények, vagy a módosított pénzforgalmi irányelv (PSD2) [2] szerinti adatait tartalmazza;

illetve

- a Távoli kulcs menedzsment szolgáltató által kezelt magánkulcs esetében a Távoli kulcs menedzsment szolgáltató;
- a *Hitelesítés-szolgáltató*.

Ezenkívül az *Előfizető*k, az *Érintett felek*, az alkalmazásszoftverek szállítói és más harmadik felek magas kockázatú tanúsítvány problémákról szóló jelentéseket nyújthatnak be, amelyekben a *Hitelesítés-szolgáltató*t értesítik a *Tanúsítvány* visszavonását igénylő okokról, mint például csalás, visszaélés vagy kulcskompromittálódás.

A *Hitelesítés-szolgáltató* honlapja egyértelmű utasításokat tartalmaz a feltételezett magánkulcs kompromittálódás, a helytelen *Tanúsítvány* használat vagy más lehetséges típusú csalás, kompromittálódás, visszaélés, nem megfelelő használat vagy a Tanúsítvánnyal kapcsolatos egyéb kérdések bejelentésére a következő webhelyen:

`https://e-szigno.hu/tanusitvany-biztonsagi-esemenyek-bejelentese.html`

3.2.2. A visszavonási kérelemre vonatkozó eljárás

A *Hitelesítés-szolgáltató* a tanúsítvány visszavonási kérelem benyújtására *Ügyfel*ei részére az alábbi lehetőségeket biztosítja:

- A *Hitelesítés-szolgáltató* honlapján keresztül a nap 24 órájában.

  A *Hitelesítés-szolgáltató* honlapján benyújtott kérelmeket a *Hitelesítés-szolgáltató* informatikai rendszere azonnal elbírálja, az elbírálás eredményéről az oldalon tájékoztatja a kérelem benyújtóját;

- elektronikus formában, a kérelmező nem álneves, a visszavonni kívánt *Tanúsítvány*nál nem alacsonyabb biztonsági besorolású *Tanúsítvány*án alapuló elektronikus aláírásával ellátva;

- elektronikus formában, az *Előfizető* – a visszavonni kívánt *Tanúsítvány*nál nem alacsonyabb biztonsági besorolású – *Tanúsítvány*ának felhasználásával létrehozott bélyegzőjével ellátva;

- papíralapon kézi aláírással ellátva a *Hitelesítés-szolgáltató* ügyfélszolgálati irodájában ügyfélszolgálati időben, vagy postai úton.

A *Hitelesítés-szolgáltató* a kérelem elbírálása során ellenőrzi a benyújtott kérelem hitelességét és a kérelmet benyújtó jogosultságát.

Érvényes elektronikus aláírással ellátott visszavonási kérelem esetében nincs szükség a kérelmező azonosságának és a kérelem hitelességének további vizsgálatára.

A papíralapon, postai úton történő visszavonási kérelem benyújtása esetében a *Hitelesítés-szolgáltató* ellenőrzi a kérelmen található kézi aláírást.

Visszavonáskor meg kell adni a visszavonás okát. Amennyiben a visszavonást az *Ügyfél* kéri, és a visszavonás okát nem adja meg, a *Hitelesítés-szolgáltató* úgy tekinti, hogy a visszavonás oka az, hogy az *Alany* a *Tanúsítvány*t a továbbiakban nem kívánja használni.

Amennyiben a visszavonást az *Ügyfél* kéri kulcskompromittálódás miatt, akkor a *Hitelesítés-szolgáltató* lehetőséget biztosít számára a visszavonási eljárás során, hogy a visszavonandó *Tanúsítvány* helyett kulcscsere keretében új *Tanúsítvány*t igényeljen.

Az írásos formában benyújtott visszavonási kérelmek esetében a *Hitelesítés-szolgáltató* lehetővé teszi, hogy a visszavonást időzítve kérjék egy későbbi dátumra.

A visszavonási kérelemnek tartalmaznia kell a *Tanúsítvány* beazonosításához szükséges adatokat.

A kérelmezőnek különösen a következő adatokat kell megadnia:

- az *Alany* pontos megnevezése;

- *Minősített elektronikus bélyegzőt létrehozó eszköz*ön kiadott *Tanúsítvány* esetében a *Minősített elektronikus bélyegzőt létrehozó eszköz* egyedi azonosítója;

- a *Tanúsítvány* egyedi azonosítója;
- A visszavonás kért dátuma, amennyiben nem azonnali visszavonást kér;
- az *Ügyfél* azonosító adatai.

Amennyiben a benyújtott visszavonási kérelem hiányos vagy érvénytelen, a *Hitelesítés-szolgáltató* elutasítja a kérelmet. Az elutasítás tényéről és okáról emailben tájékoztatja az *Alany*t és az *Előfizető*t.

Érvényes, hiánytalan kérelem esetén a *Hitelesítés-szolgáltató* dönt a kérelem elfogadásáról és a kért visszavonási időpont függvényében azonnal visszavonja a *Tanúsítvány*t, vagy beállítja a kérelemben megadott napot az időzített visszavonás időpontjaként.

Sikeres visszavonás esetén a *Hitelesítés-szolgáltató* emailben értesíti az *Alany*t és az *Előfizető*t a visszavonás tényéről.

A visszavonásról és a felfüggesztésről további információ található a a *Hitelesítés-szolgáltató* alábbi web oldalán:

`https://e-szigno.hu/tanusitvany-felfuggesztese-es-visszavonasa.html`

Tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentése

A *Hitelesítés-szolgáltató* egy folyamatosan elérhető 24/7 belső ügyeletet tart fenn a tanúsítvánnyal kapcsolatos problémák sürgősségi bejelentésére.

A *Hitelesítés-szolgáltató* a bejelentés átvételétől számított 24 órán belül megkezdi a kivizsgálást és döntést hoz a visszavonás indokoltságáról az alábbi szempontok figyelembe vételével:

- a bejelentett probléma jellege;
- a visszavonás következményei;
- az adott Tanúsítvánnyal vagy *Előfizető*vel kapcsolatban kapott bejelentések száma;
- a bejelentést tevő személy vagy szervezet;
- vonatkozó jogi szabályozás.

A *Hitelesítés-szolgáltató* megküldi a vizsgálat eredményét tartalmazó előzetes jelentést az érintett *Előfizető*nek és a bejelentést tévő személynek.

Minden körülmény alapos mérlegelése után a *Hitelesítés-szolgáltató* az *Előfizető* és a bejelentést tévő személy bevonásával eldönti, hogy visszavonja-e a *Tanúsítvány*t, és ha igen, akkor milyen időpontban.

A bejelentés átvételétől a visszavonási állapot változás publikálásáig eltelt idő nem lépheti túl a *Szolgáltatási szabályzat* 4.9.5 fejezetében meghatározott időkorlátot.

Amennyiben indokolt, a *Hitelesítés-szolgáltató* megküldi a Nemzeti Média- és Hírközlési Hatóság részére is a kivizsgálás eredményét tartalmazó jelentést.

3.2.3. A végfelhasználói tanúsítványok

A *Hitelesítés-szolgáltató* által kibocsátott végfelhasználói *Tanúsítvány*ok érvényességi ideje:

- legfeljebb a kibocsátástól számított 2 év;
- nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók;
- nem haladhatja meg a *Tanúsítvány*t kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejét.

A tanúsítvány megújítás keretében a végfelhasználói kulcshoz kibocsátható új *Tanúsítvány*.

A *Tanúsítvány*ok és a magánkulcsok érvényességi idejét befolyásolhatja, ha a Nemzeti Média- és Hírközlési Hatóság új algoritmusokkal kapcsolatos határozatot ad ki, amely szerint a felhasznált kriptográfiai algoritmus vagy kulcsparaméter már nem biztonságos a kibocsátáskor tervezett felhasználási idő végéig.

Amennyiben ez bekövetkezik, a *Hitelesítés-szolgáltató* visszavonja az érintett *Tanúsítvány*okat.

4. A megfelelőség vizsgálata

A *Hitelesítés-szolgáltató* tevékenységét az Európai Uniós szabályozással összhangban a Nemzeti Média- és Hírközlési Hatóság felügyeli. A Nemzeti Média- és Hírközlési Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart a *Hitelesítés-szolgáltató* telephelyén. A helyszíni ellenőrzés előtt a *Hitelesítés-szolgáltató* külső auditor igénybevételével átvilágíttatja üzemeltetését és az átvilágításról készült részletes megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül a Nemzeti Média- és Hírközlési Hatóságnak benyújtja. Az átvizsgálás során azt kell megállapítani, hogy a *Hitelesítés-szolgáltató* működése megfelel-e az eIDAS Rendeletben [1] és a vonatkozó magyar jogszabályokban megállapított követelményeknek, valamint az alkalmazott *Hitelesítési rend*(ek)ben és az ennek megfelelő *Szolgáltatási szabályzat*(ok)ban támasztott követelményeknek.

Az átvilágítás tematikája és módszertana megfelel az alábbi normatív dokumentumoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];

- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [8]
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [7]
- ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [9]
- ETSI EN 319 411-2 v2.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; [10]

A megfelelőségértékelési vizsgálat eredménye bizalmas dokumentum, csak az arra jogosultak számára hozzáférhető.

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt a *Hitelesítés-szolgáltató* honlapján közzéteszi.

A *Hitelesítés-szolgáltató* vizsgált és tanúsított elemeket (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz a szolgáltatásaihoz kapcsolódóan.

Az *Alany*ok részére a *Hitelesítés-szolgáltató* a következő *Minősített elektronikus bélyegzőt létrehozó eszköz*öket biztosíthatja:

- IDPrime MD 840 (kontaktusos) és IDPrime MD 3840 (kontaktusos és kontaktus mentes) intelligens kártya, amely M7820 A11 mikrochipből, MultiApp v3 Java Card platformból és IAS v.4 elektronikus aláíró alkalmazásból áll
  (Gyártó: Gemalto)

- IDPrime MD 940 (kontaktusos) és IDPrime MD 3940 (kontaktusos és kontaktus mentes) intelligens kártya, amely M7892 G12 mikrochipből, MultiApp v4.0.1 Java Card platformból és MOC v1.1 szerveren futó IAS Classic v.4.4.2 elektronikus aláíró alkalmazásból áll
  (Gyártó: Gemalto)

Távoli kulcsmenedzsment szolgáltatás esetén:

- Eszköz: Trident version 2.1.3

  (Gyártó: I4P.informatikai Kft. (I4P Ltd.))

Kivezetés alatt álló eszközök

Az alábbi *Minősített elektronikus bélyegzőt létrehozó eszköz*ök a 2022 végére tervezett kriptográfiai algoritmus váltás miatt fokozatosan kivezetésre kerülnek. A *Hitelesítés-szolgáltató* már nem rendelkezik ilyen típusú kibocsátható eszközökkel, így semmilyen esetben sem történik új eszközön *Tanúsítvány* kibocsátás és ehhez kapcsolódó kulcs előállítás.

A korábban kibocsátott és még használatban lévő *Minősített elektronikus bélyegzőt létrehozó eszköz*ökre a *Hitelesítés-szolgáltató* továbbra is bocsáthat ki új *Tanúsítvány*okat a korábban az eszközhöz kibocsátott *Tanúsítvány*ok megújítása, módosítása során, és folyamatosan biztosítja az eszközök használatához szükséges szoftver komponenseket és támogatást.

- Intelligens kártya, amely ST19WR66I mikrochipből és Touch & Sign2048 V1.00 aláíró alkalmazásból áll.
  (Gyártó: ST Incard)

- MultiApp ID Citizen 72k intelligens kártya, amely S3CC91C mikrochipből, MultiApp v1.1 Java Card platformból és IAS Classic v.3.0 elektronikus aláíró alkalmazásból áll.
  (Gyártó: Gemalto)

- IDClassic 340 intelligens kártya, amely P5CC081V1A mikrochipből, MultiApp ID v2.1 Java Card platformból és IAS Classic v.3 elektronikus aláíró alkalmazásból áll (verzió: MPH117 V2.2 szűrővel).
  (Gyártó: Gemalto)

A *Hitelesítés-szolgáltató* a *Minősített elektronikus bélyegzőt létrehozó eszköz* használatba vételét megelőzően meggyőződik róla, hogy az az aktuális követelményeknek megfelelő érvényes eszköz tanúsítvánnyal rendelkezik.

A *Hitelesítés-szolgáltató* a *Minősített elektronikus bélyegzőt létrehozó eszköz*t teljes életciklusa alatt az eszköz tanúsítvány mellékletében található követelményeknek megfelelően kezeli.

A *Hitelesítés-szolgáltató* folyamatosan figyeli a használt *Minősített elektronikus bélyegzőt létrehozó eszköz*ök tanúsítottsági állapotát legalább az azokon kibocsátott utolsó *Tanúsítvány* érvényességi idejének végéig és a tanúsítottsági állapot változása esetén megteszi a szükséges lépéseket.

A *Minősített elektronikus bélyegzőt létrehozó eszköz* tanúsítvány visszavonása esetén a *Hitelesítés-szolgáltató* visszavonja az adott *Minősített elektronikus bélyegzőt létrehozó eszköz*ön kibocsátott összes olyan *Tanúsítvány*t, amelyekben fel volt tüntetve a "id-etsi-qcs 4" nyilatkozat

A *Hitelesítés-szolgáltató* által használt *Minősített elektronikus bélyegzőt létrehozó eszköz*ök aktuális listája és a tanúsításukkal kapcsolatos információ megtalálható a *Hitelesítés-szolgáltató* honlapján az alábbi linken:

https://e-szigno.hu/kripto-eszkozok-tanusitottsaga.html

A tanúsított *Minősített elektronikus bélyegzőt létrehozó eszköz*ök tájékoztató jellegű teljes listája megtalálható az Európai Bizottság honlapján. [5]

A *Hitelesítés-szolgáltató* a szolgáltatások nyújtásához használt valamennyi rendszerelemet biztonsági osztályokba sorolta kockázatmenedzsment rendszere alapján. Ezen rendszerelemekről és a hozzájuk tartozó biztonsági besorolásról a *Hitelesítés-szolgáltató* a kockázatmenedzsment rendszere keretében nyilvántartást vezet.

A *Hitelesítés-szolgáltató* a külső auditon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely segítségével rendszeresen vizsgálja a korábbi auditoknak való megfelelőséget és eltérés esetén megteszi a szükséges lépéseket.

A *Hitelesítés-szolgáltató* 2002 óta rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási, valamint 2003 óta a ISO/IEC 27001-nek (korábban BS 7799-nek) megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet (Lloyd's Register Quality Assurance) auditál és vizsgál felül folyamatosan (lásd: 1.3. fejezet).

A vonatkozó jogszabályokról és megfelelőségi auditokról további információ található a jelen dokumentum 5.4 fejezetében és a *Szolgáltatási szabályzat* 8. és 9.15 fejezeteiben.

5. Egyéb üzleti és jogi kérdések

5.1. Tevékenységért viselt felelősség és helytállás

5.1.1. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

Az *Előfizető* felelősségét a Szolgáltatási szerződés és annak mellékletei (köztük az Általános szerződési feltételek) határozzák meg.

Az *Előfizető* kötelezettségei

Az *Előfizető* köteles a *Hitelesítés-szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során, beleértve a *Tanúsítvány*ok és magánkulcsok igénylését és alkalmazását.

Az *Előfizető* kötelezettségeit a jelen *Szolgáltatási szabályzat*, a Szolgáltatási szerződés és annak elválaszthatatlan részét képező Általános Szerződési Feltételek, valamint a vonatkozó *Hitelesítési rend* tartalmazzák.

[5] https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

Amennyiben az *Előfizető* tudomására jut, hogy az *Előfizető*höz tartozó valamely *Tanúsítvány* nyilvános kulcsához tartozó magánkulcs kompromittálódott vagy a kompromittálódás gyanúja felmerült, az *Előfizető* köteles

- e tényt haladéktalanul jelezni a *Hitelesítés-szolgáltató*nak,
- kezdeményezni a *Tanúsítvány* felfüggesztését vagy visszavonását,
- megszüntetni a *Tanúsítvány*hoz tartozó magánkulcsok használatát.

Az *Előfizető* jogai

Az *Előfizető* jogosult:

- a szolgáltatások igénybevételére a jelen *Szolgáltatási szabályzat*ban leírtak szerint;
- írásban meghatározni, hogy mely *Alany* kaphasson tanúsítványt;
- a *Tanúsítvány*ok felfüggesztését és visszavonását kérni;
- *Szervezeti ügyintéző*ket kijelölni.

Az *Igénylő* felelőssége

Az *Igénylő* felelős:

- a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért;
- a *Tanúsítvány*ában szereplő adatok ellenőrzéséért,
- az adataiban bekövetkezett változások haladéktalan bejelentéséért;
- *Elektronikus bélyegzőt létrehozó eszköz*ének, magánkulcsának és *Tanúsítvány*ának a szabályzatoknak megfelelő felhasználásáért;
- magánkulcsának és aktivizáló kódjának biztonságos kezeléséért;
- a *Hitelesítés-szolgáltató* haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben;
- általában a kötelezettségei betartásáért.

Az *Igénylő* kötelezettségei

Az *Igénylő* köteles:

- a szolgáltatás igénybevétele előtt megismerni a jelen *Szolgáltatási szabályzat*ot;
- a *Hitelesítés-szolgáltató* által kért, a szolgáltatás igénybevételéhez szükséges adatokat hiánytalanul megadni, a valóságnak megfelelő adatokat szolgáltatni;
- amennyiben az *Igénylő* tudomására jut, hogy az általa megadott, a szolgáltatás igénybevételéhez szükséges adat – különösen valamely *Tanúsítvány*ban is szereplő adat – megváltozott, haladéktalanul köteles:
  - erről írásban értesíteni a *Hitelesítés-szolgáltató*t,
  - kérni a *Tanúsítvány* felfüggesztését vagy visszavonását és
  - megszüntetni a *Tanúsítvány* használatát;
- haladéktalanul megszüntetni a *Tanúsítvány* használatát,

  amennyiben az *Igénylő* tudomására jut, hogy az általa igényelt *Tanúsítvány*t visszavonták, vagy a kibocsátó CA magánkulcsa kompromittálódott;
- a szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a hivatkozott szabályzatokban és dokumentumokban foglaltaknak megfelelően használni;
- biztosítani, hogy a szolgáltatás igénybevételéhez szükséges adatokhoz és eszközökhöz (jelszavakhoz, titkos kódokhoz, aláírás-létrehozó eszközökhöz) illetéktelen személyek ne férhessenek hozzá;
- a *Hitelesítés-szolgáltató*t haladéktalanul írásban értesíteni, amennyiben valamely a szolgáltatással kapcsolatos elektronikus bélyegzővel, illetve Tanúsítvánnyal kapcsolatban jogvita indul;
- együttműködni a *Hitelesítés-szolgáltató*val

  a *Tanúsítvány* kiadásához szükséges adatok ellenőrzése érdekében,

  és mindent megtenni azért, hogy az ellenőrzés a lehető leghamarabb befejeződhessen;
- kulcs kompromittálódás vagy nem jogszerű használat gyanújának felmerülése esetében a *Hitelesítés-szolgáltató* megkereséseire

  a *Hitelesítés-szolgáltató* által megadott időn belül reagálni;
- tudomásul venni, hogy az *Előfizető* jogosult a *Tanúsítvány* visszavonását vagy felfüggesztését kérni;

- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a *Tanúsítvány*t a *Szolgáltatási szabályzat*ban leírt meghatározott módon, az ott leírt ellenőrzési lépések elvégezése után bocsátja ki;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* a kibocsátott *Tanúsítvány*okban kizárólag a valóságnak megfelelő adatokat szerepeltet. Ennek megfelelően a *Hitelesítés-szolgáltató* a *Tanúsítvány*ba kerülő adatokat a *Szolgáltatási szabályzat* szerint ellenőrzi;
- tudomásul venni, hogy a *Hitelesítés-szolgáltató* jogosult a kibocsátott *Tanúsítvány*t azonnal felfüggeszteni illetve visszavonni, amennyiben
  - tudomására jut, hogy a *Tanúsítvány*ban foglalt adatok nem felelnek meg a valóságnak, vagy a magánkulcs nem az *Igénylő* kizárólagos birtokában vagy használatában van, és ebben az esetben az *Igénylő* köteles a *Tanúsítvány* használatát beszüntetni;
  - az *Előfizető* megszegi a Szolgáltatási szerződés vagy az Általános Szerződési Feltételek feltételeit,
  - a visszavonást megköveteli a a *Hitelesítés-szolgáltató Hitelesítési rend*je vagy *Szolgáltatási szabályzat*a;
  - a *Hitelesítés-szolgáltató* tudomására jut, hogy a *Tanúsítvány*t illegális tevékenységhez használták;
  - az *Előfizető* nem fizeti meg határidőre a szolgáltatások díját.

Az *Igénylő* jogai

Az *Igénylő* jogosult:

- *Tanúsítvány*t igényelni a jelen *Szolgáltatási szabályzat*ban leírtak szerint;
- *Tanúsítvány*ának felfüggesztését, illetve visszavonását kérni jelen *Szolgáltatási szabályzat* szerint, amennyiben ezt a vonatkozó *Hitelesítési rend* lehetővé teszi.

5.1.2. Az Érintett fél felelőssége

Az *Érintett felek* saját belátásuk és/vagy szabályzataik alapján dönthetnek az egyes *Tanúsítvány*ok elfogadásáról és a felhasználás módjáról. Az érvényesség vizsgálata során a *Hitelesítés-szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, ezért különös tekintettel javasolt:

- a *Hitelesítési rend*ben és a *Szolgáltatási szabályzat*ban megfogalmazott követelmények, előírások betartása;

- megbízható informatikai környezet és alkalmazások használata;
- a *Tanúsítvány* visszavonási állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján;
- a *Tanúsítvány* felhasználására vonatkozó valamennyi korlátozás figyelembevétele, amely a *Tanúsítvány*ban, a a *Szolgáltatási szabályzat*ban és a vonatkozó *Hitelesítési rend*ben szerepel.

5.2. A felelősség korlátozása

- A *Hitelesítés-szolgáltató* nem felelős az olyan károkért, amelyek abból adódnak, hogy az *Érintett fél* a *Tanúsítvány*ok ellenőrzése és felhasználása során nem a hatályos jogszabályok és a *Hitelesítés-szolgáltató* szabályzatai szerint ajánlottan járt el, illetve nem úgy járt el, ahogyan az az adott helyzetben elvárható.
- A *Hitelesítés-szolgáltató* a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helytállni.
- A *Hitelesítés-szolgáltató* nem felelős az abból adódó károkért, amikor valamely külső, elháríthatatlan esemény miatt az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.
- Amennyiben a *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátása előtt adategyeztetést végez egy közhiteles adatbázissal, az onnan kapott adatokat hitelesnek fogadja el.

  A *Hitelesítés-szolgáltató* nem vállal felelősséget ezen közhiteles adatbázis által szolgáltatott információk pontatlanságából eredő károkért.
- A *Hitelesítés-szolgáltató* kizárólag azért vállal felelősséget, hogy a szolgáltatásokat a jelen *Szolgáltatási szabályzat*ban, illetve az abban meghivatkozott dokumentumokban (*Hitelesítési rend*ek, szabványok, ajánlások) leírtaknak, valamint saját belső szabályzatainak megfelelően nyújtja.

Adminisztratív folyamatok

A *Hitelesítés-szolgáltató* a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) a naplóadatokat.

A *Hitelesítés-szolgáltató* az archivált adatokat az alábbi időtartamokig őrzi meg:

- a *Hitelesítési rend*et a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított legalább 10 évig;
- Általános Szerződési Feltételeket a hatályon kívül helyezéstől számított legalább 10 évig;
- videotechnológiás személyazonosítás esetén az azonosítás során rögzített teljes kommunikációt legalább a rögzítés időpontjától számított 10 évig;
- a *Tanúsítvány*okkal kapcsolatos valamennyi elektronikus és/vagy papír alapú információt legalább
  - a *Tanúsítvány* érvényességének lejáratától számított 10 évig;
  - a Tanúsítvánnyal előállított elektronikus bélyegzővel kapcsolatos jogvita jogerős lezárásáig;
- minden egyéb archiválandó dokumentomot a keletkezésétől számított legalább 10 évig.

Pénzügyi felelősség

A *Hitelesítés-szolgáltató* pénzügyi felelőssége, valamint a megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében a jogszabályi előírásoknak megfelelő óvadékkal rendelkezik.

A *Hitelesítés-szolgáltató* a megbízhatóság biztosítása érdekében a jogszabályi előírásoknak megfelelő felelősségbiztosítással rendelkezik.

Pénzügyi felelősség korlátozása

A *Hitelesítés-szolgáltató* nem korlátozza az egy alkalommal vállalható legmagasabb kötelezettség mértékét.

A minősített szolgáltatóként nyújtott szolgáltatásokkal kapcsolatban a *Hitelesítés-szolgáltató* díjcsomagokat határoz meg, amelyek a *Hitelesítés-szolgáltató* pénzügyi felelősségének mértékében térnek el egymástól az alábbiak szerint:

Tanúsítványtípus	Szolgáltatói felelősségvállalás korlátja [mFt]
alap	0,02
bronz	0,1
ezüst	5
arany	20
platina	200

Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

5.3. Vitás kérdések rendezése

A *Hitelesítés-szolgáltató* törekszik a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét követi.

A *Hitelesítés-szolgáltató* és az *Ügyfél* kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalanul értesítsen és teljes körűen tájékoztasson az ügy minden vonatkozását illetően.

Az *Ügyfél* vitás kérdés felmerülése esetén jogosult az esetleges bírósági eljárást megelőzően a Budapesti Békéltető Testülethez fordulni.

A *Hitelesítés-szolgáltató* tevékenységével vagy a kiadott *Tanúsítvány*ok felhasználásával kapcsolatos kérdéseket, kifogásokat és panaszokat az ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 3 munkanapon belül a *Hitelesítés-szolgáltató* értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a *Hitelesítés-szolgáltató* köteles írásban válaszolni a bejelentőnek. A *Hitelesítés-szolgáltató* a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől. A *Hitelesítés-szolgáltató* a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt.

Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a *Hitelesítés-szolgáltató* bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a *Hitelesítés-szolgáltató*val és az *Érintett felek*kel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 10 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a *Hitelesítés-szolgáltató* válaszát és egyéb szükséges információkat tartalmazó dokumentumokat.

Amennyiben az egyeztetés a panasz benyújtásától számított 30 napon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az *Érintett felek* kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság, illetve a Fővárosi Törvényszék kizárólagos illetékességének.

5.4. Irányadó jog

A *Hitelesítés-szolgáltató* tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A *Hitelesítés-szolgáltató* szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

A. Hivatkozások

[1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről .

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2015/2366 IRÁNYELVE (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről .

[3] 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról .

[4] 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról .

[5] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[6] 541/2020. (XII. 2.) Korm. rendelet a bizalmi szolgáltatások esetében a személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerekről

[7] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[8] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.

[9] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[10] ETSI EN 319 411-2 v2.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;.

[11] Magyarország (Hungary): Trusted List (`http://www.nmhh.hu/tl/pub/HU_TL.pdf`).

[12] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti minősített elektronikus bélyegző tanúsítvány hitelesítési rendek.

[13] Microsec zrt. - Tájékoztató az online videóazonosítás feltételeiről .